Capstone Project

Migrating the SECDEF Communications Team to the Cloud

Final Report

MPTM 900-201, Capstone, Georgetown University

Professor: Dr. Maria Trujillo

Lenny Reekoye - Ryan Shimek

Spring 2019

Table of Contents

Abstract

The Secretary of Defense controls the three combat branches of the United States armed forces while at home and abroad. One of the primary purposes of the office is to build, strengthen, and maintain U.S. relations with other nations and their Defense Ministers. This means that the Secretary is often away from the Pentagon and requires extensive deployed communication capabilities in order to perform his duties. The 844th Communications Squadron (CS), located at Joint Base Andrews, is responsible for ensuring that the Secretary of Defense and Deputy Secretary of Defense have those communications capabilities while on the road. To provide this support, the 844th CS deploys ahead of the Secretary and establishes a communications room to be utilized while in the area. In order to complete their mission, the 844th CS personnel require access to data that is currently located on legacy servers located at the Pentagon. The team's goal with this project is to build a new data solution using cloud technology in order to replace the legacy servers (which will remain as backups to the cloud). This will create a new continuity of operations plan (COOP) for the 844th CS to ensure that they are able to support the Secretary of Defense`s mission needs.

Problem Statement

The data utilized by the 844th Communications Squadron to complete their missions in support of the Secretary of Defense and Deputy Secretary of Defense currently resides on legacy servers in the Department of Defense at the Pentagon. While there have been no instances of inability to access this data, there is currently no feasible continuity plans in place. If the data were to become inaccessible while the Secretaries was traveling, it would degrade the mobile communication abilities and potentially cause harm to our national security.

The 844th CS provides rapidly deployable, interoperable, and scalable command and control (C2) systems supporting a common set of Joint C2 capabilities and integrated applications and hardware for SECDEF and DEPSECDEF support.

When advancing ahead of the delegation, the communications teams are responsible for setting up a communications room, which includes a network stack that reaches back to the Pentagon, computers, phones, TEMPEST (emanations) equipment and more. After in-depth research, which includes speaking with personnel who support the mission, examining past trip reports, and through obtaining a basic understanding of the SECDEF's duties, data usage, access to the data located at the Pentagon servers has been identified as a main cause of concern. Their job is to ensure the Secretaries are able to communicate with the President and other top officials. The 844th CS personnel uses the data on the legacy servers in the greater Washington D.C area and worldwide. They utilize past trip reports and briefings to plan upcoming trips, coordinate with the Pentagon's Advance Officers, and with U.S. embassies located all around the world. When deployed, the teams use the data to troubleshoot any hardware issues, provide reports and intelligence to the delegation, and also keep up to date with ongoing worldwide operations.

If this data were to become inaccessible, the 844th CS would be unable to successfully complete their mission in support of the SECDEF and DEPSECDEF communication efforts. In order to ensure this does not occur, a secure and reliable, yet accessible worldwide cloud solution will mitigate many of these concerns, while also ensuring that the data remained available.

The mission of the SECDEF and DEPSECDEF include working to build international relations, while also maintaining their duties of protecting the United States and its people. If these missions were to fail it during a national crisis or world crisis, such as an attack on the U.S. similar to 9/11 attacks, it would greatly delay the response time of our Secretaries and top officials and ultimately causing greater harm to our national security interest.

Project Scope

The Department of Defense (DoD) is charged with managing and overseeing all functions of the government concerned directly with national security interests and the United States Armed Forces. The National Defense Strategy of 2018, written by former Secretary of defense Jim Mattis emphasizes a long-term strategic approach and priority of resources in order to become a more lethal force with the reform of the DoD for greater performance and affordability. The scope of the project will be to build a new data solution using cloud technology in order to replace the legacy servers (which will remain as backups to the cloud). This technology will create a new continuity of operations plan (COOP) for the 844th CS to ensure the unclassified data is protected and continuous support of the SECDEF`s mission. “Almost half of the government organizations are actively using cloud services.” (Garther. 2018). Overall Information technology budget can be reduced by approximately 15-20% if the

cloud migration is a successful. We expect the implementation of this project will take 3-5 years for approval and to complete the full migration into the cloud.

The "What If" Scenario

(Please note, this scenario is completely fictional, any similarities to real world situations are purely coincidental.)

The 844th travel team is currently deployed to three different European sites and have established a communications suite at each site. The SECDEF is set to arrive at location one within the next few minutes and the team at the site has just been notified that the connection to the Pentagon servers have been lost and the repair won't be completed for another hour. At the same time, a foreign enemy has just attacked one of the United State's allies and their Defense Minister is requesting to speak with the SECDEF.

Due to the connection being lost with the Pentagon servers, the SECDEF is unable to receive any real-time intelligence on the situation. The Defense Minister is demanding the U.S. to take action against the aggressors, but without the proper actionable intelligence at his disposal, the SECDEF is morally unable to issue any orders against the enemy. This, in turn, causes a fallout with the U.S ally as they lose trust and faith in the abilities of the U.S to aid and strike in their time of need.

Research

Many government organizations and agencies have already migrated or have begun migrating to cloud technology. With our research, the team will explore the benefits of cloud technology and why it is the ideal solution for 844th CS continuity plans. Also, the team hopes to learn not only from other organizations' successes but also their failures. Cloud migrations from different the U.S Army and more will be visited and studied in order to better understand the process and uncover the best way forward for the 844th CS.

Why the Cloud?

There are a number of reasons why companies are switching to the cloud today and the most important, at least from the 844th CS' perspective, is availability. "Most cloud providers are extremely reliable in providing their services, with many maintaining 99.99% uptime. The connection is always on and as long as workers have an Internet connection, they can get to the applications they need from practically anywhere. Some applications even work offline" (Coles, 2018, par. 8).

Another huge benefit to new technology solutions for any government organization is one that can also help cut costs. In an article from Digital Reality, Okey Keke writes about ways cloud technologies can cut costs and states that "as cloud computing has evolved, two major changes have happened for organizations and their IT expenditures. First, the onset of virtualization means that hardware expense has decreased drastically. Second, the proliferation of cloud and interconnection services means that deploying services/applications is easier than ever and organizations do not have to spend weeks or months ordering and configuring connectivity to access them" (Keke, 2017, par. 3). Also, along with cutting down on hardware costs, it also allows organizations to greatly reduce their data footprint by reducing the size of

their data centers. With this comes the opportunity to cut costs of your workforce as you will no longer need the same number of technicians managing the work centers.

Finally, another great benefit that goes hand-in-hand with availability and the 844th CS' mission is improved mobility. "Data and applications are available to employees no matter where they are in the world" (Coles, 2018, par. 10). With the worldwide mission that the Secretary of Defense has, this benefit is a must, and in support of this mission, the 844th CS will have no issues accessing the data that is so critically necessary.

Government/DoD Stance on Cloud Migration

For government and military organizations, there will never be an adoption of new technologies without the backing of the DoD policy makers and top officials. Luckily for the sake of this upgrade and others like it, the DoD and U.S. government are currently urging strong pushes toward cloud migration.

The Pentagon itself is urging its organizations to start pursuing cloud migration. "The Pentagon has ordered Defense organizations that operate more than 100 of its data centers to begin migrating their applications to milCloud 2.0, the new on-premises commercial cloud service managed by the Defense Information Systems Agency" (Serbu, 2018, par 1).
Former Defense Secretary James Mattis was adamant the DoD started modernizing their Information technology (IT) practices as well. He has gone on record having stated, "The Pentagon has ordered Defense organizations that operate more than 100 of its data centers to begin migrating their applications to milCloud 2.0, the new on-premises commercial cloud service managed by the Defense Information Systems Agency" (Terry, 2018, par 9).

United States Army Migration

The U.S Army has spent a couple of years and an extensive amount of money on cloud migration and have documented many lessons learned in their pursuit of modernization. In an article from Defense Systems.com, Caroline Mohan was able to interview the Army's chief data officer, Thomas Sasala. The issues they faced ranged "from data vulnerability to limited connectivity to lack of specialized talent" (Mohan, 2018, par. 1).

In the article, they also list five strategies, the U.S Army is using to combat challenges with their cloud migration. These include establishing environments, setting a destination, incentivizing, lowering barriers, and setting conditions. For security and access, they have contracted many different cloud vendors that support the common access card, which is a security token used by the vast majority of government agencies. With the strategy of setting a destination, the U.S Army was also able to develop a well thought out business plan, which listed step-by-step processes of how to arrive toward their desired solution.

Another potential issue the U.S Army had to consider during the modernization, many of their programs and applications were previously built on legacy systems and likely would not work on new infrastructure and platform. "Modernization is the refactoring or consolidation of legacy software programming to align it more closely with current business needs. In this case, modernizing systems/applications to migrate to commercial cloud hosting environments" (Military and Aerospace, 2018, par 13).

Solution Development

The 844th CS requires a critical link for communications support for some of the highest levels of leaders in the government. They provide a mobile connection suite, which includes data, voice, and video in order to link up back to the DoD. Currently, the communication connection goes from the deployed team to the servers at the Pentagon then back to the deployed team. Worst case scenario involves the team being unable to connect to the servers. Taking into account the numerous deployments and unique mission of the 844th CS, the strict IT requirements and policies coming from the Joint Authorization Board (JAB), Office of Management and Budget (OMB), FedRAMP Program Management Office (PMO), Department of Homeland Security (DHS) and National Institute for Standards and Technology (NIST). The best solution for the Continuity of Operations (COOP) plan will be migrating to cloud technology and infrastructure. Cloud technology is part of DoD strategic objectives for cyber readiness within the federal government.

Cloud Solution Comparison

In this era of technology and computing, there are many different cloud solutions and most boast extensive benefits and capabilities. While there are many options available, not all are suitable for government or meet the strict requirements necessary for protecting the data. Without an approval system in place, picking an appropriate solution would prove difficult for any government organization. Luckily, FedRAMP has established a system to assess these solutions, and after a comprehensive process, they approve only the solutions that meet the strictest requirements. According to FedRAMP.com, there are currently 134 authorized solutions, while another 73 are currently undergoing the authorization process. For this project,

the team has decided to look at three major providers which include: IBM Cloud for Government, Microsoft Azure Government, and Amazon's GovCloud.

IBM Cloud for Government

IBM has been a world leader in technology solutions for decades, so it was no surprise to see their cloud technology listed as one of FedRAMP's authorized vendors. IBM boasts a wide array of options to fit any cloud solution needed, including being public, dedicated, private, managed, and more. Also, the IBM cloud is an open source platform, which would allow an organization the flexibility in developing a solution that directly fits their needs. IBM also claims that the "IBM Cloud supports all major government standards and regulations to help agencies move applications to the cloud with confidence, backed by multiple, overlapping tiers of protection" (IBM.com, n.d.). This is critical for the type of data that the 844th utilizes. According to Forbes, IBM is currently listed as the 3rd best cloud provider, behind Microsoft and Amazon. In that article, Bob Evans states, " IBM plays in all three layers of the cloud—IaaS, PaaS and SaaS—which is hugely important for the elite cloud vendors because it allows them to give customers more choices, more seamless integration, better cybersecurity, and more reasons for third-party developers to rally to the IBM Cloud" (Evans, 2017, par 6).

Microsoft Azure Government

In the same Forbes article that ranks IBM as #3, they rank Microsoft as the top cloud provider. "Microsoft remains an absolute lock at the top due to four factors: its deep involvement at all three layers of the cloud (IaaS, PaaS and SaaS); its unmatched commitment to developing and helping customers deploy AI, ML and Blockchain in innovative production environments" (Evans, 2017, par 4). Microsoft Azure also boasts world-class security and provides a way to

modernize legacy infrastructures. Microsoft remains a leader in the IT world and its software solutions have been critical to military and governmental advancements.

As of 2017, Microsoft has been working with the government in order to provide services that will enable them to handle classified data. “Taking the next step forward in meeting the mission-critical and data needs of our U.S. Government customers, we are announcing expansion plans to make Azure Government Secret available to support government agencies and partners who have Secret classified data. Azure Government Secret will deliver multi-tenant cloud infrastructure and cloud capabilities to U.S. Federal Civilian, Department of Defense, Intelligence Community, and U.S. Government partners working within Secret enclaves. Customers with Secret requirements can expect to gain access to new technologies at scale, including services such as cognitive capabilities, artificial intelligence, and predictive analytics” (Keane, 2017, par 4).

Azure, however, does not use availability zones similar to Amazon’s. Their availability strategy was brought into question when a storm erupted near one of their data centers. “Lightning during a powerful storm caused a voltage swell in the utility feeds powering one of the Azure data centers in San Antonio, Texas, that overwhelmed the facility’s surge suppressors, knocking out its cooling systems” (Sverdlik, 2018, par 2). This outage affected 40 Azure services

and lasted nearly 3 hours. Outages such as this one could greatly impact the 844th CS mission.

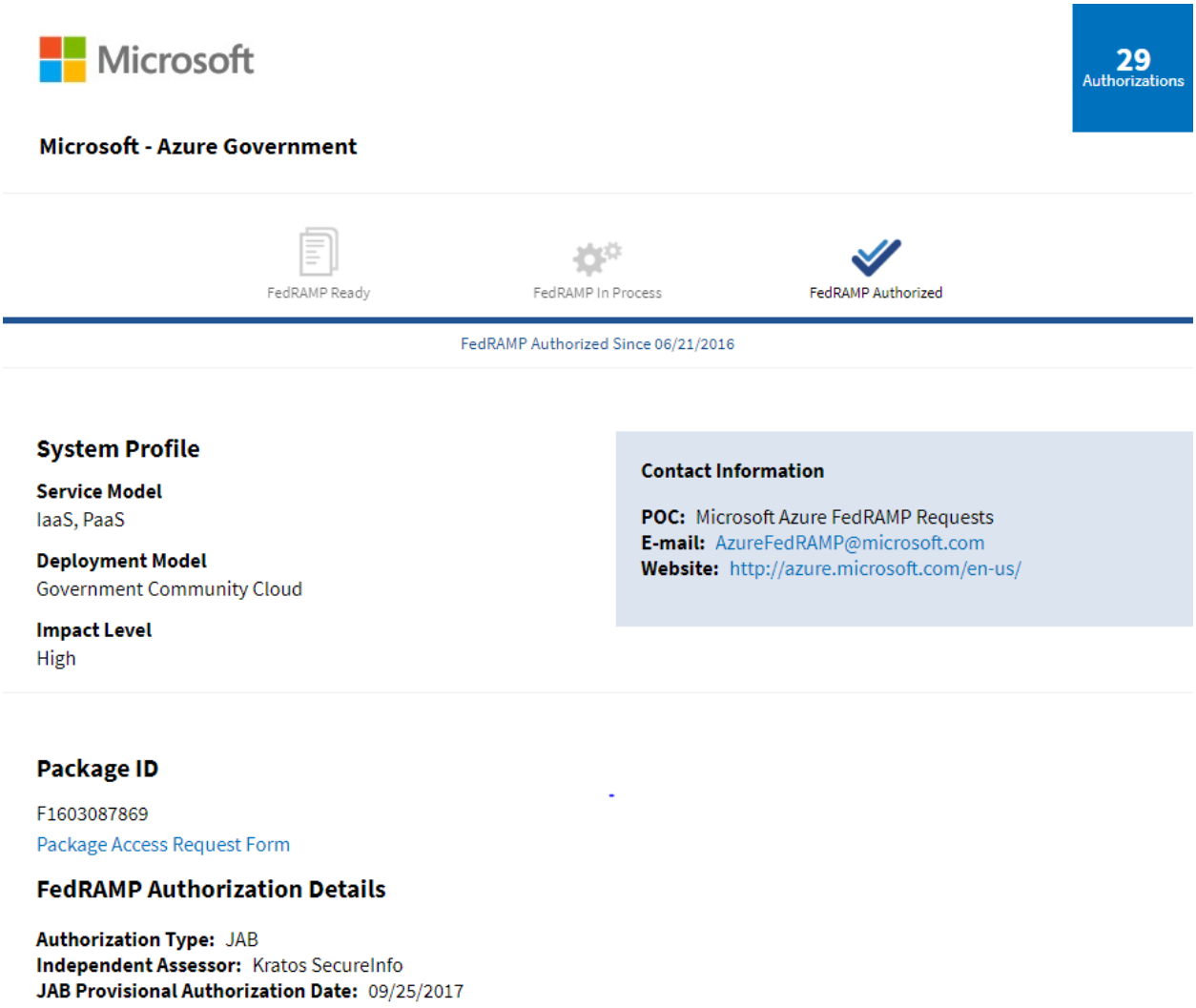

Figure 1. Microsoft Azure Government (FedRAMP, 2019)

Amazon GovCloud

Early in 2019, Canalys analyzed the current market share standings of all cloud providers and Amazon Web Services (AWS) far outpaces the competition with a 32.2% market share (figure 1). To compare, the next runner up is Microsoft Azure coming in at 13.7%. What this shows is that AWS is not only the world leader in cloud services but is also the most trusted. Not

only is AWS FedRAMP approved, but Amazon also claims that they are “the only cloud service provider with accredited regions to address the full range of DoD data classifications, including Unclassified, Sensitive (CUI), Secret, and Top Secret” (Amazon, n.d.). The team believes this is a huge accomplishment as it shows just how much the military and government trusts the security build into AWS GovCloud. AWS also boasts one of the best uptimes for all cloud services. “Since the start of 2015, AWS has had a total of 448 minutes of downtime” (McLaughlin & Sullivan, 2017, par 2.). This statistic is likely the most important in regards to the 844th mission as data availability is key to their success.

Canalys estimates: Full-year 2018

Vendor	2018 (US$ billion)	2018 Market share	2017 (US$ billion)	2017 Market share	Annual growth
AWS	25.4	31.7%	17.3	31.5%	+47.1%
Microsoft Azure	13.5	16.8%	7.4	13.5%	+82.4%
Google Cloud	6.8	8.5%	3.5	6.4%	+93.9%
Alibaba Cloud	3.2	4.0%	1.7	3.0%	+91.8%
IBM Cloud	3.1	3.8%	2.6	4.7%	+17.6%
Others	28.3	35.2%	22.4	40.8%	+26.1%
Total	**80.4**	**100.0%**	**54.9**	**100.0%**	**+46.5%**

Figure 2. Worldwide Cloud Infrastructure Spending and Annual Growth (Canalys, 2019)

Proposed Solution

After evaluating the three different cloud options, the team has concluded that Amazon’s GovCloud is the best option for the 844th’s cloud migration. While all the clouds are outstanding products, Amazon is the only cloud provider that is accredited to host all levels of classified information and proves that it is the most secure product on the market as well as the most viable for government and military use. Though there are currently no plans to migrate any classified

data to the cloud, the fact that Amazon provides this capability will allow the 844th to explore that possibility in the near future if they chose to do so.

Moreover, Amazon's reported uptimes are extremely impressive and provide the access that is needed for the proposed solution. Currently, the 844th personnel are required to Virtual Private Network (VPN) into the Pentagon servers in order to access critical data, but when using Amazon's GovCloud, they will be able to access the data through open channels. This solution, along with keeping the current legacy servers as backups will ensure that the 844th CS are able to complete their mission in providing deployed communications for the Secretary of Defense.

The team also believes and recommends that the solution consists of a hybrid cloud architecture. AWS GovCloud fully supports a hybrid implementation plan. "In cloud computing, the hybrid cloud refers to the use of both on-premises resources in addition to public cloud resources. A hybrid cloud enables an organization to migrate applications and data to the cloud, extend their datacenter capacity, utilize new cloud-native capabilities, move applications closer to customers, and create a backup and disaster recovery solution with cost-effective high availability" (Amazon, n.d., par 1). This will enable the 844th to utilize the legacy systems that are already in place as part of the backup solution.

844 CS Cloud Migration S.W.O.T. Analysis

Strengths

1. Provides 844th CS with new data backups
2. Provides 844th with fully supported worldwide data access
3. Decrease overall cost of per deployment

Weaknesses

1. Takes complete control away from 844 CS/Pentagon technicians
2. Potential harm to operations security in the event of data breach

Opportunities

1. Allows future exploration of moving classified data to the cloud
2. Lessons Learned can apply for future projects

Threats

1. Leadership might deny project based upon added security risks
2. Leadership might deny solution based upon budget
3. Third party actors may hindered the uplink connections

Business Analysis/Business Need

The business aspect of this project aligns with the DOD strategic objectives for cyber readiness within Federal government guidelines. “we must ensure the U.S. military’s ability to fight and win wars in any domain, including cyberspace. This is a foundational requirement for U.S. national security and a key to ensuring that we deter aggression, including cyber-attacks that constitute a use of force, against the United States, our allies, and our partners. The Department must defend its own networks, systems, and information from the malicious cyber activity and be prepared to defend when directed, those networks and systems operated by non-DoD Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) entities.” (DOD, Cyber Strategy Summary, 2018).

The 844th CS COOP and the project is part of the defense strategy to create a contingency plan and modernize the current systems. Increasing the resilience and deterring cyber-attacks on the 844th CS system, a cloud solution brings the security needed and the robust

infrastructure to the 844th CS without major cost or need to build from the ground up. A Cloud solution can be broken down into 3 types models; Cloud (third-party involvement), Hybrid and government private cloud. FedRamp provided information such as risk analysis, system assessment plans, security vulnerabilities, and security authorization package. FedRamp bridges the gap between Federal government and cloud providers making security priorities.

Mission Model

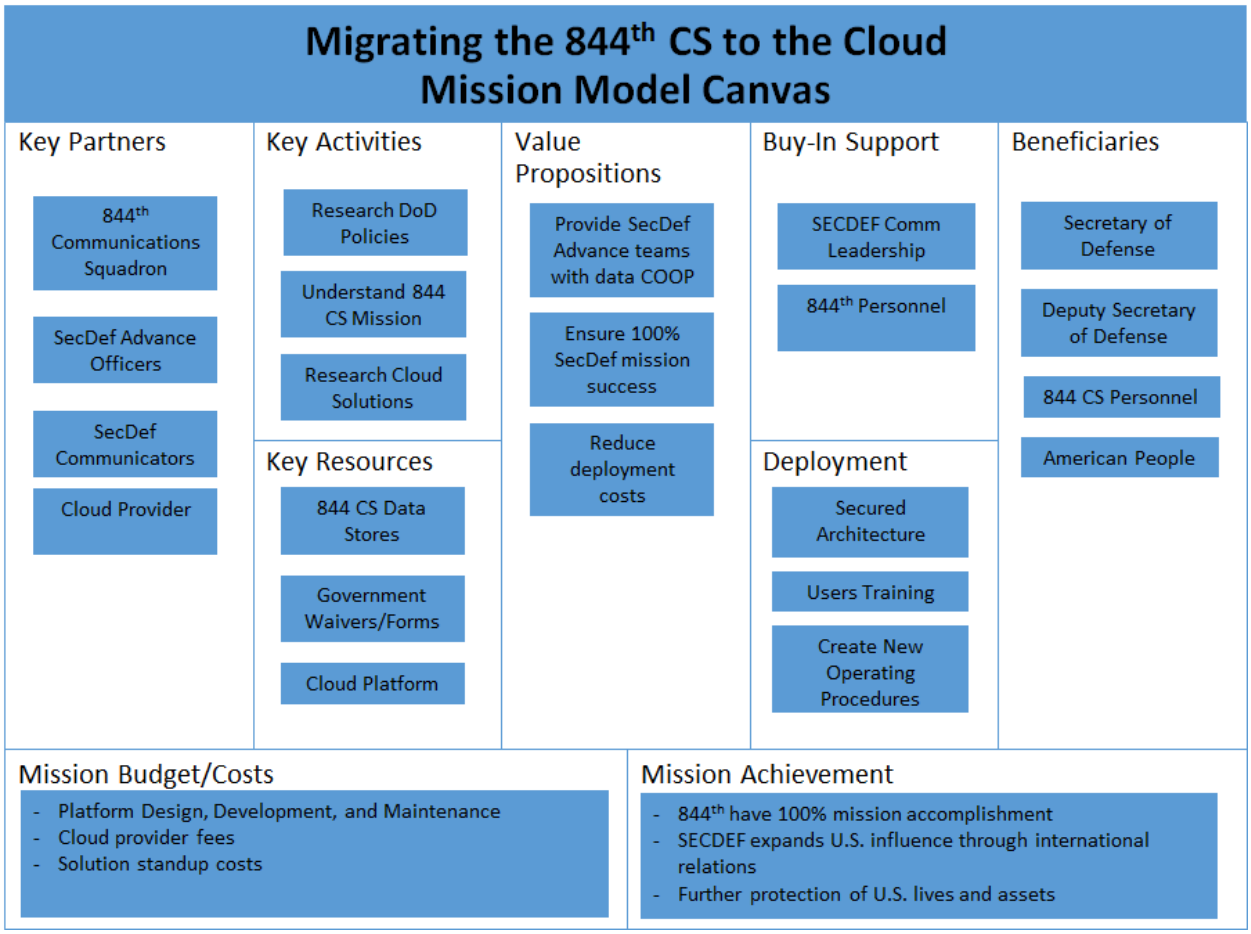

Figure 3. Business Model Canvas

Technical Architecture

Choosing to go with a third party cloud provider ultimately means that the 844th CS will not be required to invest in upgrading their infrastructure. However, it is still important to understand the capabilities of the provider and know what type of architecture the data will be hosted on.

Amazon has actually built multiple data centers in different regions of the United States (West and East). “Teresa Carlson, AWS vice president of the worldwide public sector, said that one of the reasons the company built a new government cloud was to let government agencies and their third-party contractors maintain duplicate copies of their data and apps. In the case that a problem occurs in one facility, the other data center facility can pick up the slack” (Vanian, 2018, par 4). This feature built into their infrastructure is a major benefit to the 844th as it provides yet another fallback to ensure data availability. In the same article, Amazon also claims that the different regions will reduce latency based upon your physical location.

Unfortunately, Amazon does not release specific details about the infrastructures that comprise their cloud data centers, but “operates at least 30 data centers in its global network, with another 10 to 15 on the drawing board. Amazon does not disclose the full scope of its infrastructure, but third-party estimates peg its U.S. data center network at about 600 megawatts of IT capacity” (Miller, 2015, par 3). The article by Miller continues to discuss the secrecy behind Amazon’s data centers, but Amazon executives Werner Vogel and James Hamilton have estimated that there could be about 5.6 million servers within all their facilities. These numbers came in 2015, and likely have risen exponentially since that time.

Assumptions

The cloud will give the 844th CS a second layer of protection for data access while deployed on the road. They will be able to confidently ensure mission success of providing communications support for the SECDEF and DEPSECDEF. The cloud will be extremely secure and all data will be protected. No data breaches will occur and operational security will always remain intact. The 844th CS will look into migrating classified data to the cloud in the near future. This solution will likely remain in place for at least the next decade.

844th CS Security Requirements

On December 15, 2014, DoD Chief Information Officer (CIO) memo regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services* defined DoD Component responsibilities when acquiring commercial cloud services **(**DoD, 2018). Federal Risk and Authorization Management Program (FedRAMP) was established after many trials and errors of learning and understanding cloud technology. FedRAMP's mission is to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the Federal Government. FedRAMP identifies clear and objective security capability requirements where possible, while also allowing the flexibility to add specific security controls and requirements necessary to meet DoD's critical mission requirements. With the complex structure of this project, unauthorized access, data corruption, infrastructure failure, and service unavailability are some of the risks connected to relinquishing the control to the third-party cloud provider.

Financial Analysis

From a financial analysis standpoint, the team looked at the financial statements from the fiscal year (FY) 18 deployments in order to analyze the cost of deploying a team and the required equipment, This, further assisted in determining the current financial situation and set of financial goals for the 844th CS. The annual budget for the 844th CS travel team is 3 million dollars, which is separate from the overall budget of the 844th unit. The travel team consists of 60 military personnel and 80 civilian performing and supporting the duties of the 844th CS mission. The travel team`s budget includes travel expresses such as hotels, food, and transportation for the teams also, the replacement of IT equipment and communications gear accounts for 35% of the annual travel budget. The return on investment will be the lowering of the cost of the replacement of IT equipment and communication gears.

Cost Estimate

Due to security reasons, the team was unable to receive the annual costs and details of the current infrastructure in place at the Pentagon, so we did our best to estimate the total costs of switching to the cloud. Amazon has a Total Cost of Ownership (TCO) Calculator that helps prospective clients see what they can expect to pay for their services. When estimating, the 844th CS would need 100 TB of data, the TCO calculator shows that they can expect to spend $130,680 over three years of ownership. As shown in figure 4, this estimate is

the sum of the costs of storage and data transfer costs.

AWS - Storage Costs

EBS Storage - Only Standard EBS used with no IOPS requirements

EBS Costs - Equivalent to On-Premises SAN environment

Starting capacity (GB)		18,432.00
Equivalent EBS storage volume		General Purpose (SSD)
Number of EBS volumes required		19
EBS volumes cost/month	$	2,304.00
Initial snapshot cost(one-time)	$	1,751.04
EBS incremental snapshots cost/month	$	-
Total EBS cost /month	$	2,304
EBS Costs (3 Yr) - no IOPS	**$**	**84,695**
EBS Costs (3 Yr.)	**$**	**93,165**
AWS Business Support (EBS)	**$**	**8,470**
Total AWS Storage Costs (3 Yr.) including support	**$**	**93,164.54**

AWS - Data Transfer Costs

Monthly Data Transfer Out (TB) 10.3

Data Transfer Costs

	US East (N. Virginia)	Tier(GB)	Monthly Cost
First 1 GB per month	$ -	1	$ -
Up to 10 TB per Month	$ 0.09	10240	$ 921.60
Next 40 TB per Month	$ 0.09	306	$ 26.00
Next 100 TB per Month	$ 0.07	0	$ -
Over 350 TB per Month	$ 0.05	0	$ -

Total monthly data transfer costs	$	948.00
AWS Business Support (data transfer)	**$**	**3,411**
Data Transfer Costs (3 Yr.) including support	**$**	**37,525**

Figure 4. Total Cost of Ownership Estimate (Amazon, 2019)

Ethical Considerations

The Department of Defense has high ethical codes and standards of integrity. The 844th CS is responsible for the implementation and administration of all aspects and in overseeing the cloud project. The 844th CS is responsible for going through the Defense Acquisition Regulations System (DARS) procurement processes and following the instruction and guidance for contracting. With the complex structure of this project, relinquishing the control to a third-party cloud provider, 844th CS will need to ensure the data is secure in the cloud; the data should be readily accessible when needed and protected from unauthorized viewing and changes. The developing COOP and cloud technology are a critical aspect of the 844th CS mission.

Also, with putting sensitive data on the cloud, the 844th will be taking a calculated risk by relinquishing full control of that data. As the data will no longer solely reside within the

Pentagon, it will open up more avenues for potential theft or breaches. Though no information that will be stored on the cloud at this time will be classified, the data could still potentially lead to hindrances of operational security. Though unlikely, in the event of a breach during mission planning, or even during a mission, it's possible that the mission could get canceled and could potentially waste thousands of dollars in travel funds, and also the opportunity for the Secretary to meet with foreign dignitaries.

The team must also look at ways we can prevent these risks or attempts to mitigate them if an issue arises. The team believes a contract needs to be in place with the vendor, which can guarantee notification if a breach were to occur. Having this notification would allow SECDEF communications leadership to determine what risks to the mission have occurred and then choose the appropriate action. Security is always a major concern, so it will be up to leadership to determine if they are willing to accept these risks, though the team believes that the security in place with the GovCloud is robust enough to prevent any issues.

Finally, The team must look at the ethical benefits that are presented with migrating the 844th to the cloud. Having a COOP in place will ensure that the SECDEF can fulfill his obligations to the American people while conducting business away from the Pentagon. The government places a lot of responsibility on the shoulders of its military members and they deserve solutions that will enable them to always successfully complete their missions. Thus, this solution will also help relieve the stress of deploying away from home by eliminating a fault in their continuity plans.

Conclusion

The personnel at the 844th Communications Squadron have a very unique and extremely important mission as they work to support the office of the Secretary of Defense. It is imperative they continue to find new and innovative ways to improve the process of deployed communications teams for the Secretaries` travel missions. Migrating to a cloud solution will ensure they have constant data availability while providing robust security to the unclassified data. Amazon's GovCloud will take them one step further into the future of computing and help them continue to improve upon their already excellent processes. This new solution will ensure they continue the excellence in mission success they have achieved as they work to support the Department of Defense's top leader.

Appendix

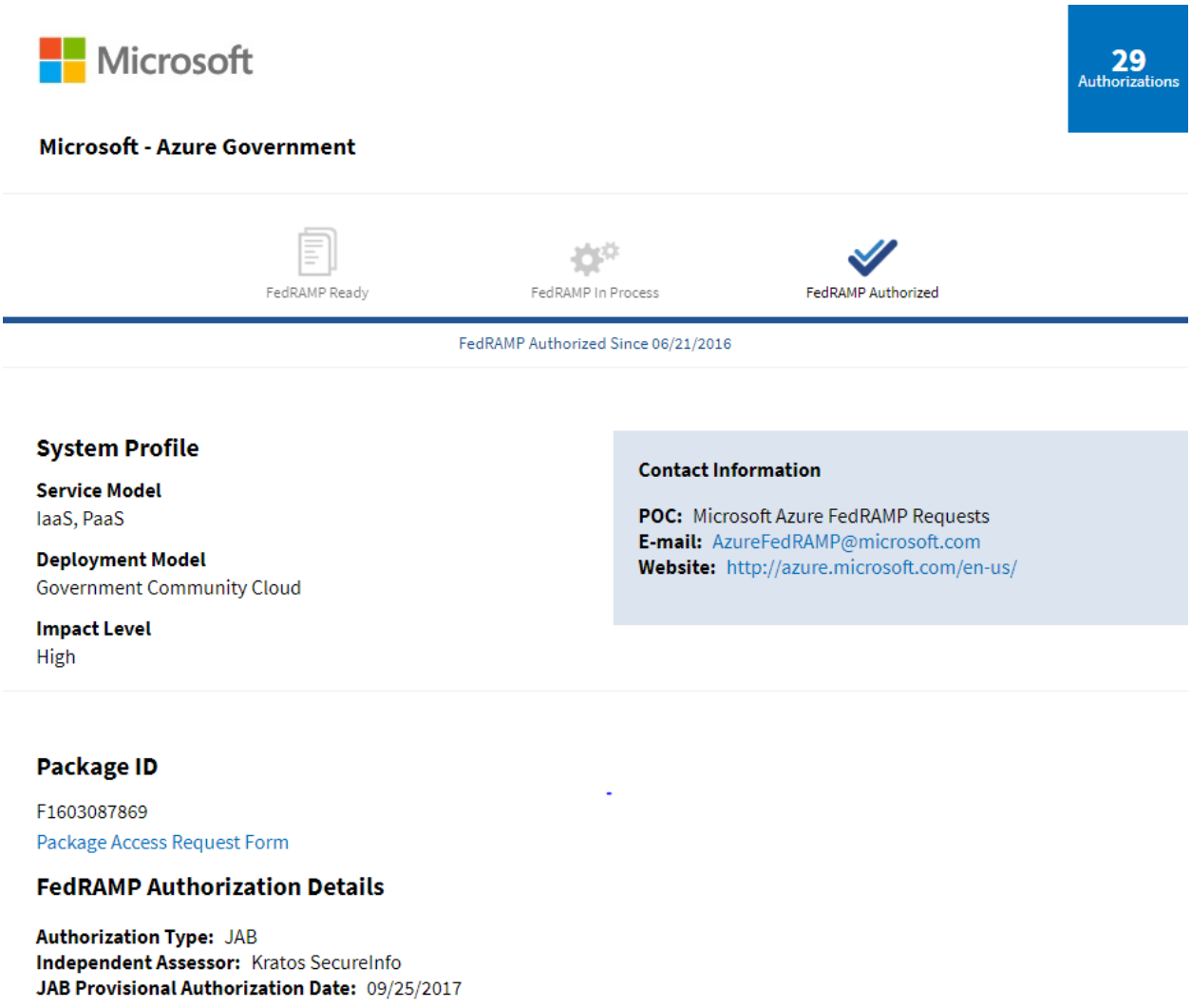

Figure 1. Microsoft Azure Government (FedRAMP, 2019)

Canalys estimates: Full-year 2018

Vendor	2018 (US$ billion)	2018 Market share	2017 (US$ billion)	2017 Market share	Annual growth
AWS	25.4	31.7%	17.3	31.5%	+47.1%
Microsoft Azure	13.5	16.8%	7.4	13.5%	+82.4%
Google Cloud	6.8	8.5%	3.5	6.4%	+93.9%
Alibaba Cloud	3.2	4.0%	1.7	3.0%	+91.8%
IBM Cloud	3.1	3.8%	2.6	4.7%	+17.6%
Others	28.3	35.2%	22.4	40.8%	+26.1%
Total	80.4	100.0%	54.9	100.0%	+46.5%

Figure 2. Worldwide Cloud Infrastructure Spending and Annual Growth (Canalys, 2019)

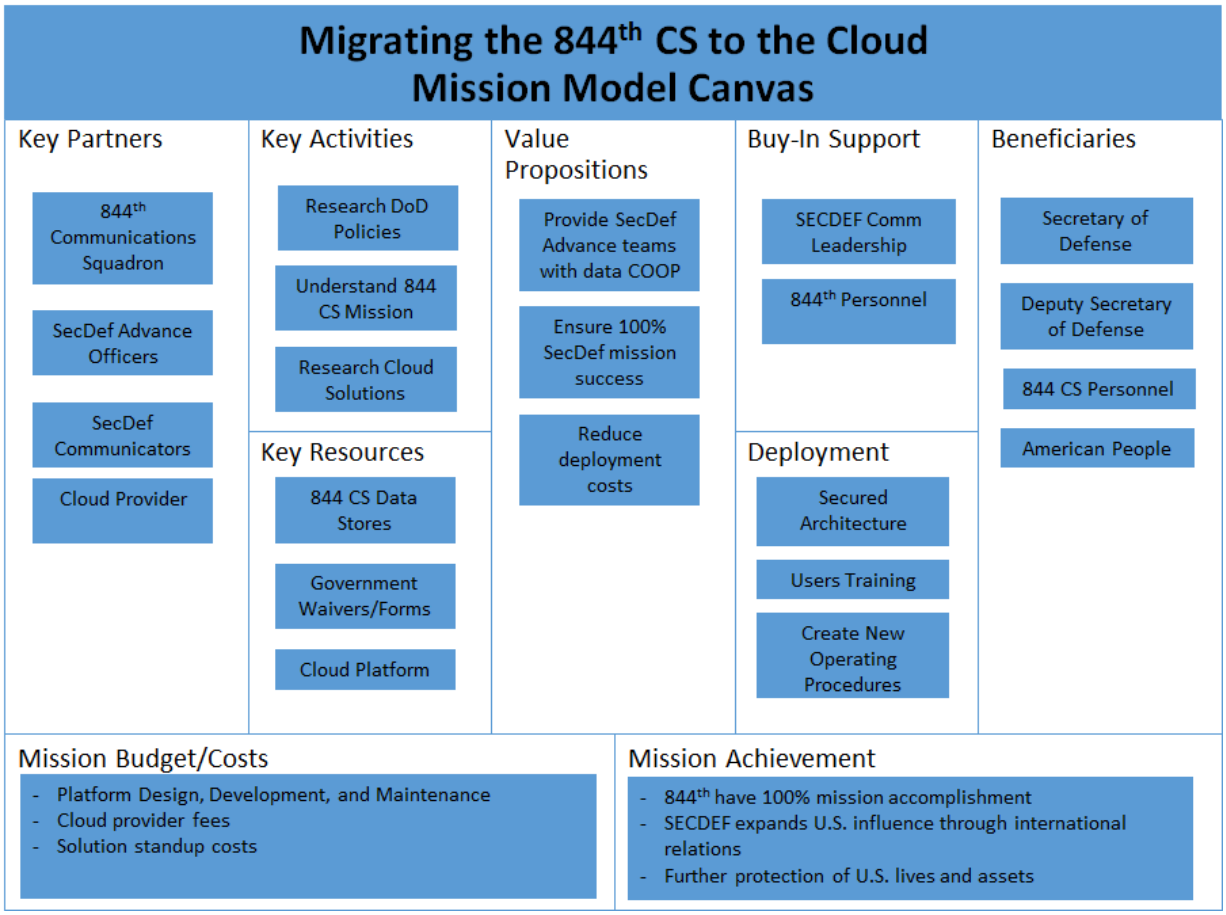

Figure 3. Mission Model Canvas

AWS - Storage Costs

EBS Storage - Only Standard EBS used with no IOPS requirements

EBS Costs - Equivalent to On-Premises SAN environment

Starting capacity (GB)		18,432.00
Equivalent EBS storage volume		General Purpose (SSD)
Number of EBS volumes required		19
EBS volumes cost/month	$	2,304.00
Initial snapshot cost(one-time)	$	1,751.04
EBS incremental snapshots cost/month	$	-
Total EBS cost /month	$	2,304
EBS Costs (3 Yr) - no IOPS	**$**	**84,695**
EBS Costs (3 Yr.)	**$**	**93,165**
AWS Business Support (EBS)	**$**	**8,470**
Total AWS Storage Costs (3 Yr.) including support	**$**	**93,164.54**

AWS - Data Transfer Costs

Monthly Data Transfer Out (TB) 10.3

Data Transfer Costs

	US East (N. Virginia)	Tier(GB)	Monthly Cost
First 1 GB per month	$ -	1	$ -
Up to 10 TB per Month	$ 0.09	10240	$ 921.60
Next 40 TB per Month	$ 0.09	306	$ 26.00
Next 100 TB per Month	$ 0.07	0	$ -
Over 350 TB per Month	$ 0.05	0	$ -

Total monthly data transfer costs	$	948.00
AWS Business Support (data transfer)	**$**	**3,411**
Data Transfer Costs (3 Yr.) including support	**$**	**37,525**

Figure 4. Total Cost of Ownership Estimate (Amazon, 2019)

References

Amazon (n.d.). Retrieved from: https://aws.amazon.com/government-education/defense/

Canalys.com. (2019, Feb 4). *Cloud Market Share Q4 2018 and Full Year 2018.* Retrieved from: https://www.canalys.com/newsroom/cloud-market-share-q4-2018-and-full-year-2018

Coles, C. (n.d.). *11 Advantages of Cloud Computing and How Your Business Can Benefit From Them.* Retrieved from: https://www.skyhighnetworks.com/cloud-security-blog/11-advantages-of-cloud-computing-and-how-your-business-can-benefit-from-them/

DoD (n.d.). Retrieved April 5, 2019, from https://iasecontent.disa.mil/cloud/SRG/index.html

Evans, B. (2017, Nov 7). *The Top 5 Cloud-Computing Vendors: #1 Microsoft, #2 Amazon, #3 IBM, #4 Salesforce, #5 SAP*. Retrieved from: https://www.forbes.com/sites/bobevans1/2017/11/07/the-top-5-cloud-computing-vendors-1-microsoft-2-amazon-3-ibm-4-salesforce-5-sap/#525c0fff6f2e

FedRAMP.gov. (n.d.). Retrieved from: https://www.fedramp.gov/

IBM.com. (n.d.). Retrieved from: https://www.ibm.com/cloud/government

Keane, T. (2017, Oct 17). *Announcing New Azure Government Capabilities for Classified Mission-Critical Workloads.* Retrieved from: https://azure.microsoft.com/en-us/blog/announcing-new-azure-government-capabilities-for-classified-mission-critical-workloads/

Keke, O. (2017, Aug 17) *How Cloud Cut Costs for IT Departments.* Retrieved from: https://www.digitalrealty.com/blog/how-cloud-cuts-costs-for-it-departments

Legacy Homepage. (n.d.). Retrieved from: https://dod.defense.gov/

McLaughlin, K. & Sullivan, M. (2017, Mar 7). *How AWS Stacks Up Against Rivals on Downtime.* Retrieved from: https://www.theinformation.com/articles/how-aws-stacks-up-against-rivals-on-downtime

Meulen, R. V. (n.d.). *Understanding Cloud Adoption in Government*. Retrieved from: https://www.gartner.com/smarterwithgartner/understanding-cloud-adoption-in-government/

Microsoft.com. (n.d.). Retrieved from: https://azure.microsoft.com

Military and Aerospace. (2018, Mar 20). *Army Modernizes, Migrates to Cloud Computing.* Retrieved from: https://www.militaryaerospace.com/articles/2018/03/u-s-army-consolidates-data-centers-while-modernizing-migrating-to-the-cloud.html

Miller, R. (2015, Sep 23). *Inside Amazon's Cloud Computing Infrastructure.* Retrieved from: https://datacenterfrontier.com/inside-amazon-cloud-computing-infrastructure/

Mohan, C. (2018, Aug 21). *Learning from the Army's Complicated Move to the Cloud.* Retrieved from: https://defensesystems.com/articles/2018/08/22/army-cloud-migration-lessons.aspx

Sverdlik, Y. (2018, Sep 12). *Azure Outage Proves the Hard Way that Availability Zones are a Good Idea.* Retrieved from: https://www.datacenterknowledge.com/microsoft/azure-outage-proves-hard-way-availability-zones-are-good-idea

Terry, R. (2018, May 14). *Here's the Pentagon's Justification to Congress for a Single Cloud Computing Contract Award.* Retrieved from: https://www.bizjournals.com/washington/news/2018/05/14/heres-the-pentagons-justification-to-congress-for.html

Vanian, J. (2018, Nov 13). *Amazon Web Services Just Opened a New Cloud for the U.S. Government*. Retrieved from: http://fortune.com/2018/11/12/amazon-web-services-govcloud/